

# INVARIANTS FOR $A_4$ FIELDS AND THE COHEN-LENSTRA HEURISTICS

SIMON RUBINSTEIN-SALZEDO

**ABSTRACT.** This article discusses deviations from the Cohen-Lenstra heuristics when roots of unity are present. In particular, we propose an explanation for the discrepancy between the observed number of cyclic cubics whose 2-class group is  $C_2 \times C_2$  and the number predicted by the Cohen-Lenstra heuristics, in terms of an invariant living in a quotient of the Schur multiplier group. We also show that, in some cases, the definition of the invariant can be simplified greatly, and we compute  $10^5$  examples.

## 1. INTRODUCTION

Cohen and Lenstra in [CL84] were interested in studying the distribution of class groups of quadratic fields, and perhaps, abelian extensions of  $\mathbb{Q}$  more generally. These heuristics were extended by Cohen and Martinet in [CM87] and [CM90] to fields of more general type.

Since class groups are finite abelian groups, we can attempt to understand them by understanding their  $p$ -Sylow subgroups. Assuming that the distributions of the  $p$ -Sylow subgroups are independent for different  $p$ , we can then patch together the distribution of class groups from the distribution of the  $p$ -Sylow subgroups for all  $p$ . (The independence of distributions at each prime is conjectural, but it is well-supported by numerical data.)

Therefore, we will restrict ourselves to looking at the distribution of the  $p$ -Sylow subgroups of the class groups of number fields. If  $K$  is a number field, we let  $\text{Cl}_p(K)$  denote the  $p$ -Sylow subgroup of  $\text{Cl}(K)$ .

In the case of quadratic fields, Cohen and Lenstra made the following conjecture:

**Conjecture 1.1** (Cohen-Lenstra). *Let  $p$  be an odd prime. Let  $D^\pm(X)$  denote the set of real (respectively imaginary) quadratic fields  $K$  with  $|\text{disc}(K)| < X$ . Let  $A$  be a finite abelian  $p$ -group. Then*

$$\lambda^\pm(A) = \lim_{X \rightarrow \infty} \frac{\#\{K \in D^\pm(X) : \text{Cl}_p(K) \cong A\}}{\#D^\pm(X)}$$

*exists, and we have*

$$\lambda^+(A) = c^+ |\text{Aut}(A)|^{-1} \times |A|^{-1}, \quad \lambda^-(A) = c^- |\text{Aut}(A)|^{-1}$$

---

*Date:* October 11, 2012.

for certain explicit constants  $c^+$  and  $c^-$ , which are independent of  $A$ .

The statement of this conjecture suggests many further questions. One such question is why we need to restrict to the case of an odd prime  $p$ . The reason is that the 2-torsion in the class group is controlled by genus theory. If  $K$  is a quadratic field and  $r$  is the number of primes dividing  $\text{disc}(K)$ , then the 2-torsion of  $\text{Cl}(K)$  is isomorphic to  $C_2^{r-1}$  or  $C_2^{r-2}$  (see [FT93], Corollary 1 to Theorem 39, for a more precise statement and a proof). In particular, the 2-torsion in quadratic fields is rarely equal to 0 and can easily become arbitrarily large.

Of course, we need not lose interest in class groups as soon as we step beyond quadratic fields: we could ask the same question for fields of other types. Furthermore, in this case, the 2-power torsion will not necessarily be governed by genus theory, so we might also allow  $p$  to be 2. So, we could make the following guess, by attempting to apply the Cohen-Lenstra heuristics to situations for which we have no *a priori* reason for believing that they are appropriate.

**Heuristic 1.2** (Proto-Cohen-Lenstra Heuristics). *Let  $n$  be a positive integer, and let  $G$  be a transitive permutation group on a set of size  $n$ . Furthermore, let  $(r_1, r_2)$  be a signature, with  $r_1 + 2r_2 = n$ . Let  $D(X)$  be the set of number fields  $K$  the absolute value of whose discriminant is less than  $X$ , and so that the Galois group  $\text{Gal}(K^\#/\mathbb{Q})$  of the Galois closure of  $K$  is isomorphic to  $G$ , and  $K$  has  $r_1$  real embeddings and  $r_2$  pairs of complex conjugate embeddings. Finally, let  $p$  be a prime not dividing  $|G|$  and let  $A$  be a finite abelian  $p$ -group. Then*

$$\lim_{X \rightarrow \infty} \frac{\#\{K \in D(X) : \text{Cl}_p(K) \cong A\}}{\#D(X)}$$

*exists, and is inversely proportional to  $|\text{Aut}(A)| \times |A|^{r_1+r_2-1}$ .*

However, the proto-Cohen-Lenstra heuristics sometimes fail for silly reasons. Here is an example:

**Lemma 1.3.** *Let  $n = 3$  and  $G = C_3$  in the above heuristics. If  $p \equiv 2 \pmod{3}$ , then the  $p$ -rank of  $K$ ,  $r_p(K) := \dim_{\mathbb{F}_p}(\text{Cl}(K)/p\text{Cl}(K))$ , is even for all such  $K$ .*

*Proof.* The Galois group  $C_3 = \{1, \sigma, \sigma^2\}$  of  $K$  over  $\mathbb{Q}$  acts on  $\text{Cl}_p(K)$ . The number of ideal classes of order  $p$  is  $p^{r_p(K)} - 1$ , which is congruent to 0 (mod 3) if and only if  $r_p(K)$  is even. Hence, if  $r_p(K)$  is odd, then there must be a nontrivial  $p$ -torsion ideal class  $C$  fixed by the Galois action. In particular, there is a nonprincipal ideal  $\mathfrak{a} \in C$  of order  $p$  so that  $\mathfrak{a}$ ,  $\mathfrak{a}^\sigma$ , and  $\mathfrak{a}^{\sigma^2}$  are all in the same ideal class. We now show that their product  $\mathfrak{a}^{1+\sigma+\sigma^2}$  is equal to the principal ideal  $(N\mathfrak{a})\mathfrak{o}_K$ . For any  $a \in \mathfrak{a}$ ,  $Na = a^{1+\sigma+\sigma^2} \in \mathfrak{a}^{1+\sigma+\sigma^2}$ , and the  $Na$  generate  $(N\mathfrak{a})\mathfrak{o}_K$  as an  $\mathfrak{o}_K$ -module, so  $(N\mathfrak{a})\mathfrak{o}_K \subset \mathfrak{a}^{1+\sigma+\sigma^2}$ . Now, the norms of both ideals  $\mathfrak{a}^{1+\sigma+\sigma^2}$  and  $(N\mathfrak{a})\mathfrak{o}_K$  are  $(N\mathfrak{a})^3$ . Hence, they are equal. Furthermore,  $(N\mathfrak{a})\mathfrak{o}_K$  is principal, since it is generated by the element  $N\mathfrak{a}$ . Hence  $C^3 = 1$  in  $\text{Cl}_p(K)$ . But this is impossible, as  $3 \nmid p$ .  $\blacksquare$

We can patch the proto-Cohen-Lenstra heuristics by excluding those  $A$  that are ruled out by this Lemma and related ones. Furthermore, as the proof of the lemma hints, for those  $A$  that are allowable, we need the automorphisms to be compatible with the Galois action, in the case that  $K$  is actually a Galois number field. In particular, if  $G = C_\ell$ , then we need  $A$  to be a  $\mathbb{Z}[\zeta_\ell]$ -module. This suggests the following refinement of the proto-Cohen-Lenstra heuristics, at least in the case where  $n = \ell$  is a prime, and  $G = C_\ell$ :

**Heuristic 1.4** (Refined Cohen-Lenstra Heuristics). *Let  $\ell$  be an odd prime, and let  $G = C_\ell$ . Let  $D(X)$  be the set of  $C_\ell$  number fields with absolute discriminant less than  $X$ . (Such fields are necessarily totally real.) Also, let  $p$  be a prime different from  $\ell$  and  $A$  an abelian  $p$ -group with the structure of a  $\mathbb{Z}[\zeta_\ell]$ -module. Then*

$$\lim_{X \rightarrow \infty} \frac{\#\{K \in D(X) : \text{Cl}_p(K) \cong A\}}{\#D(X)}$$

*exists, and is inversely proportional to  $|\text{Aut}_{\mathbb{Z}[\zeta_\ell]}(A)| \times |A|^{\ell-1}$ .*

Another, more modern and sometimes cleaner, way to interpret the refined Cohen-Lenstra heuristics is based on the following idea from probability theory. Let  $\mu$  be a probability distribution on  $\mathbb{R}$ . Define the  $k^{\text{th}}$  moment of  $\mu$  to be

$$a_k = \int_{-\infty}^{\infty} x^k d\mu.$$

From knowing the sequence of moments  $a_1, a_2, \dots$ , it is possible to reconstruct  $\mu$  under fairly mild hypotheses. To be more precise, define the moment generating function to be the power series

$$A(x) = \sum_{k=1}^{\infty} a_k \frac{x^k}{k!}.$$

Then assuming that  $A(x)$  has positive radius of convergence,  $\mu$  is the only probability distribution having moment generating function  $A(x)$ . (See [Bil95], Chapter 30, for a proof.)

In the context at hand, we can define an analogue of a moment for a probability distribution  $f$  of finite abelian  $p$ -groups as follows. Fix a finite abelian  $p$ -group  $A$ , and look at the expected number of surjections (in whichever category is appropriate) from an  $f$ -random finite abelian  $p$ -group  $X$  to  $A$ . This number behaves as the “ $A^{\text{th}}$  moment of  $X$ .” Just as in the situation for classical moments of probability distributions, these  $A^{\text{th}}$  moments of  $X$  determine  $f$ , assuming that  $f$  is fairly well-behaved.

We now put this in proper context. If  $A$  is a finite abelian  $p$ -group that also has the structure of a  $\mathbb{Z}[\zeta_\ell]$ -module, then we would like to understand the number

$$\mathbb{E}(\#\text{Surj}_{\mathbb{Z}[\zeta_\ell]}(\text{Cl}(K), A)).$$

Here  $\text{Surj}$  is the set of surjective maps, and  $\mathbb{E}$  denotes the expected value. Let us look at the case of  $n = 3$  and  $G = C_3$ . Then the refined Cohen-Lenstra heuristics are

equivalent to

$$(1.1) \quad \lim_{X \rightarrow \infty} \frac{1}{\#D(X)} \sum_{K \in D(X)} p^{r_p(K)} = \begin{cases} \left(1 + \frac{1}{p}\right)^2 & p \equiv 1 \pmod{3}, \\ 1 + \frac{1}{p^2} & p \equiv 2 \pmod{3}. \end{cases}$$

In the case when  $A = C_p$  (if  $p \equiv 1 \pmod{3}$ ) or  $A = C_p \times C_p$  (if  $p \equiv 2 \pmod{3}$ ), then

$$\mathbb{E}(\# \text{Surj}_{\mathbb{Z}[\zeta_3]}(\text{Cl}(K), A)) = \lim_{X \rightarrow \infty} \frac{1}{\#D(X)} \sum_{K \in D(X)} (p^{r_p(K)} - 1).$$

So, in particular, if  $p = 2$ , we would expect the number of surjections from the class group of a random  $C_3$  field to  $C_2 \times C_2$  to be  $1/4$ . As we shall see shortly, however, this appears not to be the case.

The goal of this article is to attempt to explain this discrepancy, noted by Malle in [Mal08] in the Cohen-Lenstra heuristics when roots of unity are present. We will focus on one case: that of  $C_3$  fields whose class groups surject onto  $C_2 \times C_2$ . It will turn out to be more convenient for us not to work directly with the  $C_3$  field; instead, class field theory associates to a surjection from the class group of a  $C_3$  field to  $C_2 \times C_2$  an  $A_4$  field; we work with this  $A_4$  field instead.

In §2, we present the results of Malle's computations and what the modifications to the Cohen-Lenstra heuristics appear to be. In order to introduce our new results and explanations, we discuss the Schur multiplier and a variant of it called the reduced Schur multiplier; this is done in §3.

The new material begins in §4. Here we present an invariant associated to an  $A_4$  field which is expected to explain the discrepancy in (2.1). In §5, we present an algorithm to compute the invariant, and we show that in certain circumstances, the invariant has a simple interpretation as the parity of the class group of a certain field. In §6, we perform an explicit computation of the invariant for the smallest  $A_4$  field. Finally, we end this article with Table 1, which summarizes the data collected from  $10^5$  fields, and a guess about a possible secondary term.

This article is adapted from the author's PhD thesis [RS12]. A reader who wishes for a slightly more leisurely exposition may prefer to read Chapters 2 and 3 of the thesis instead.

## 2. MALLE'S COMPUTATIONS

**Notation.** We use the following notation: for  $q, k \in \mathbb{N}$ , let

$$(q)_k = \prod_{i=1}^k (1 - q^{-i}), \quad (q)_\infty = \prod_{i=1}^{\infty} (1 - q^{-i}).$$

After performing many tests, Malle proposed a list of cases in which the Cohen-Lenstra heuristics are expected to fail. In particular, when  $p = 2$ , they should always

fail. In the case of  $C_3$  fields, the Cohen-Lenstra heuristics predict that the Sylow 2-subgroup of the class group should be isomorphic to  $C_2 \times C_2$  with probability

$$\frac{1}{12} \frac{(4)_\infty}{(4)_1} \approx .0765.$$

Instead, in his sample of over 16 million fields, he finds that the actual probability is closer to .13, nearly twice as large as expected. Similarly, equation (1.1) does not seem to hold when  $p = 2$ : equation (1.1) predicts that the average size of the maximal elementary abelian 2-subgroup of  $\text{Cl}(K)$  be  $\frac{5}{4}$ , but Malle's computations suggest that the correct number is  $\frac{3}{2}$ .

In terms of expected number of surjections, it appears that

$$(2.1) \quad \mathbb{E}(\# \text{Surj}_{\mathbb{Z}[\zeta_3]}(\text{Cl}(K), C_2 \times C_2)) = 1/2,$$

rather than  $1/4$ , as mentioned in the previous section.

In general, Malle expects the Cohen-Lenstra heuristics to fail at the prime  $p$  when the ground field contains  $p^{\text{th}}$  roots of unity. In this case, he expects that if  $A$  is a nontrivial abelian  $p$ -group, then  $\text{Cl}_p(K) \cong A$  more often than the Cohen-Lenstra heuristics predict.

**Remark 2.1.** For  $C_3$  fields, the Cohen-Lenstra prediction also fails for  $p = 3$ , since the 3-torsion in the class group is governed by genus theory, just as in the case of  $p = 2$  for quadratic fields. More generally, the Cohen-Lenstra predictions at a prime  $p$  do not hold for fields with Galois group  $G$  if  $p$  divides  $|G|$  because of genus theory. In this article, we are not especially interested in the failure for that reason, since genus theory is well-understood. Thus, we will only be concerned with deviations due to the existence of  $p^{\text{th}}$  roots of unity.

### 3. SCHUR MULTIPLIERS AND VARIANTS

Our proposed correction to the Cohen-Lenstra heuristics in the presence of roots of unity can be described in terms of the reduced Schur multiplier. We first recall the definition of the Schur multiplier, then move on to the reduced Schur multiplier.

**Definition 3.1.** Let  $G$  be a group.

- (1) The Schur multiplier group of  $G$  is defined to be the second homology group  $H_2(G, \mathbb{Z})$ .
- (2) A central extension of  $G$  is a short exact sequence

$$0 \rightarrow A \rightarrow \tilde{G} \rightarrow G \rightarrow 1,$$

where  $A$  is an abelian group, and  $A$  is contained in the center of  $\tilde{G}$ .

- (3) A stem extension of  $G$  is a central extension

$$0 \rightarrow A \rightarrow \tilde{G} \rightarrow G \rightarrow 1$$

so that  $A$  is contained in the intersection of the center of  $\tilde{G}$  and the derived subgroup of  $\tilde{G}$ .

If  $G$  is finite, there is a stem extension  $\tilde{G}$  of maximal order; in fact, there may be more than one of maximal order, and such  $\tilde{G}$  need not be isomorphic. However, as  $\tilde{G}$  varies over maximal stem extensions, the corresponding  $A$  are all isomorphic, and they are isomorphic to the Schur multiplier group  $H_2(G, \mathbb{Z})$ . If, in addition,  $G$  is a perfect group (i.e.,  $G = [G, G]$  is its own commutator subgroup), then there is a unique such group  $\tilde{G}$ .

Suppose  $G$  is a finite group. Then  $H_2(G, \mathbb{Z})$  is a finite group all of whose elements have order dividing the order of  $G$ . Also, for a prime  $p$ , the Sylow  $p$ -subgroup of  $H_2(G, \mathbb{Z})$  is trivial if the Sylow  $p$ -subgroup of  $G$  is cyclic. For convenience, we provide a few examples of Schur multiplier groups.

**Proposition 3.2.** (1) (Schur 1907, also Corollary 2.2.12 in [Kar87]) Let  $G$  be the finite abelian group

$$G \cong C_{n_1} \times C_{n_2} \times \cdots \times C_{n_k},$$

with  $n_{i+1} \mid n_i$  for  $1 \leq i \leq k-1$ . Let  $C_n^{(m)}$  denote the direct product of  $m$  copies of  $C_n$ . Then

$$H_2(G, \mathbb{Z}) \cong C_{n_2} \times C_{n_3}^{(2)} \times \cdots \times C_{n_k}^{(k-1)}.$$

(2) Let  $G = C_2 \times C_2$ . Then  $H_2(G, \mathbb{Z}) \cong C_2$ . There are two maximal stem extensions of  $G$ :

$$0 \rightarrow C_2 \rightarrow D_8 \rightarrow C_2 \times C_2 \rightarrow 0$$

and

$$(3.1) \quad 0 \rightarrow C_2 \rightarrow Q_8 \rightarrow C_2 \times C_2 \rightarrow 0.$$

(3) Let  $G = A_n$  be the alternating group on  $n$  letters. Then

$$H_2(G, \mathbb{Z}) = \begin{cases} 1 & n \leq 3, \\ C_2 & n \geq 4 \text{ and } n \neq 6, 7, \\ C_6 & n = 6, 7. \end{cases}$$

If  $n = 4$ , then we have  $A_4 \cong \text{PSL}_2(\mathbb{F}_3)$ , and the unique maximal stem extension of  $A_4$  is

$$(3.2) \quad 0 \rightarrow C_2 \rightarrow \text{SL}_2(\mathbb{F}_3) \rightarrow A_4 \rightarrow 1.$$

Furthermore, the sequence (3.1) is the sequence of Sylow 2-subgroups of (3.2). If  $n = 5$ , we have  $A_5 \cong \text{PSL}_2(\mathbb{F}_5)$ , and the unique maximal stem extension of  $A_5$  is

$$0 \rightarrow C_2 \rightarrow \text{SL}_2(\mathbb{F}_5) \rightarrow A_5 \rightarrow 1.$$

We write  $\tilde{A}_n$  for the maximal stem extension of  $A_n$ .

(4) Let  $G = S_n$  be the symmetric group on  $n$  letters. Then

$$H_2(G, \mathbb{Z}) = \begin{cases} 1 & n \leq 3, \\ C_2 & n \geq 4. \end{cases}$$

For  $n \geq 4$ , there are two nonisomorphic double covers of  $S_n$ .

In fact, what we really need is not the full Schur multiplier group, but a certain quotient of it, associated to a certain union of conjugacy classes of  $G$ . To this end, fix a union of conjugacy classes  $c \subset G$ . Let

$$0 \rightarrow H_2(G, \mathbb{Z}) \rightarrow \tilde{G} \rightarrow G \rightarrow 1$$

be a Schur cover. Suppose  $x \in c$  and  $y \in G$  commute. Lift  $x$  and  $y$  to  $\tilde{x}$  and  $\tilde{y}$ , respectively, in  $\tilde{G}$ . (This can be done in multiple ways; choose one arbitrarily.) Then the commutator  $[\tilde{x}, \tilde{y}]_{\tilde{G}}$  lies in  $H_2(G, \mathbb{Z})$ , and this element is independent of the choice of lifts. Call this element  $\langle x, y \rangle_{\tilde{G}}$ . Let  $Q_c$  denote the subgroup of  $H_2(G, \mathbb{Z})$  generated by all the  $\langle x, y \rangle_{\tilde{G}}$ 's.

**Definition 3.3.** The reduced Schur multiplier of a pair  $(G, c)$  is the quotient

$$H_2(G, c, \mathbb{Z}) = H_2(G, \mathbb{Z})/Q_c.$$

A reduced Schur cover of  $(G, c)$  is the quotient  $\tilde{G}_c = \tilde{G}/Q_c$ .

A reduced Schur cover is a largest stem extension of  $G$  so that  $c$  lifts bijectively to a union of conjugacy classes  $\tilde{c} \subset \tilde{G}_c$ .

**Remark 3.4.** We will tend to be slightly sloppy with our terminology when referring to reduced Schur covers. In the future, when we refer to a reduced Schur cover  $\tilde{G}_c$ , we shall assume that it comes packaged with a union of conjugacy classes  $\tilde{c} \subset \tilde{G}_c$  which bijects onto  $c$ , even when no explicit choice of  $\tilde{c}$  is provided.

**Example.** Suppose  $G = A_5$ . If  $c$  is the conjugacy class of 3-cycles, then  $H_2(G, c, \mathbb{Z}) \cong C_2$ , and the corresponding extension is

$$0 \rightarrow C_2 \rightarrow \tilde{A}_5 \rightarrow A_5 \rightarrow 1.$$

However, if  $c$  is the conjugacy class of  $(12)(34)$ , then  $H_2(G, c, \mathbb{Z})$  is trivial.

#### 4. INVARIANTS FOR NUMBER FIELDS

We now introduce the invariant of Ellenberg and Venkatesh as described in [VE10]. This will be an attempt to explain (2.1), as follows: Ordinarily, we would expect the right-hand side of (2.1) to be  $1/4$ , but in this case, it is twice as large as we anticipate. To each surjection  $\varphi : \text{Cl}(K) \twoheadrightarrow C_2 \times C_2$  of  $\mathbb{Z}[\zeta_3]$ -modules, we associate an invariant  $\mathfrak{z}(\varphi) \in \{0, 1\}$ . We then hope that

$$\mathbb{E}(\#\{\varphi \in \text{Surj}_{\mathbb{Z}[\zeta_3]}(\text{Cl}(K), C_2 \times C_2) : \mathfrak{z}(\varphi) = 0\}) = \frac{1}{4}$$

and

$$\mathbb{E}(\#\{\varphi \in \text{Surj}_{\mathbb{Z}[\zeta_3]}(\text{Cl}(K), C_2 \times C_2) : \mathfrak{z}(\varphi) = 1\}) = \frac{1}{4}.$$

(For convenience, we will overuse the notation  $\mathfrak{z}$  a little bit: sometimes, we will write  $\mathfrak{z}(\varphi)$  to denote the invariant of a surjection, and sometimes we will write  $\mathfrak{z}(\rho)$  to denote the invariant of a field corresponding to a representation  $\rho : G_K \rightarrow C_2 \times C_2$ .)

The motivation for this comes from the case of function fields, which was studied by Ellenberg, Venkatesh, and Westerland in [EVW09]. In this case, the extensions are parametrized by a Hurwitz space, which may have several connected components. On each connected component, the number of extensions agrees (asymptotically) with the Cohen-Lenstra predictions, but there is a discrepancy when there are multiple connected components. This is discussed at the end of [EVW12]. In the number field case, we have no Hurwitz space to parametrize the extensions, but we are left with a vestige of the connected components, which are given in terms of the Schur multiplier.

We now consider the following scenario, which is a modification of that considered by Ellenberg and Venkatesh in [VE10]. Let  $K$  be a number field or function field, let  $G$  be a finite group, and let  $c = c_1 \cup \dots \cup c_r \subset G$  be a union of conjugacy classes. Then, we assume that the following conditions hold:

- Conditions 4.1.**
- (1)  $G$  has trivial center.
  - (2)  $c$  generates  $G$ .
  - (3) If  $n$  is prime to the order of an element  $g \in c$ , then  $g^n \in c$ .

**Example.** These conditions hold if  $G = A_4$  and  $c$  is the union of the two conjugacy classes of 3-cycles. They also hold if  $G = A_5$  and  $c$  either the conjugacy class of 3-cycles or the conjugacy class of a product of two disjoint 2-cycles.

**Lemma 4.2** (Ellenberg-Venkatesh). *Let  $K$  be a totally real number field, let  $G$  be a finite group, and let  $c$  be a union of conjugacy classes of  $G$ , satisfying Conditions 4.1 above, and let  $\rho : G_K \rightarrow G$  be a homomorphism so that*

- (1)  $\rho$  is trivial at all infinite places.
- (2)  $\rho$  is tamely ramified, and the image of each inertia group  $I_{\mathfrak{p}}$  in  $G_K$  is a cyclic subgroup contained in  $c \cup \{1\}$ .

*Furthermore, we assume that  $2H_2(G, c, \mathbb{Z}) = 0$ . Then  $\rho$  lifts to an extension  $\tilde{\rho} : G_K \rightarrow \tilde{G}_c$  which is trivial at all infinite places and tamely ramified.*

**Remark 4.3.** The conclusion of the Lemma is sometimes still valid even when the hypotheses are not all satisfied. In particular, if  $G = C_2 \times C_2$  and  $c$  consists of just the identity, the conclusion still holds, even though  $c$  does not generate  $G$ . This particular case will show up again shortly.

We may now define the invariant  $\mathfrak{z}(\rho) \in H_2(G, c, \mathbb{Z})$ . If  $H_2(G, c, \mathbb{Z}) = 0$ , set  $\mathfrak{z}(\rho) = 0$ . Otherwise, assume that  $H_2(G, c, \mathbb{Z}) \neq 0$ . For each finite place  $v$  of  $K$ , let  $\mathfrak{p}_v$  be the corresponding prime and  $k_v$  the residue field at  $v$ , and let  $q_v$  be the size of  $k_v$ . Let



$I_v$  be the inertia group of  $G_K$  at  $v$ , and fix an element  $\pi \in \mathfrak{p}_v - \mathfrak{p}_v^2$ . We have a map  $I_v \rightarrow k_v^\times$ , given by  $\sigma \mapsto \sigma(\pi)/\pi \pmod{\mathfrak{p}_v}$ . Let  $g_v$  be any inverse image of  $-1$  so that  $g_v$  topologically generates a subgroup of  $I_v^{\text{tame}}$  of index  $\frac{q_v-1}{2}$ . Now, each  $x \in c$  is the image of a unique  $x^* \in \tilde{c}$ .

**Definition 4.4.** The invariant  $\mathfrak{z}(\rho)$  is defined to be

$$(4.1) \quad \mathfrak{z}(\rho) = \prod_{v \text{ finite}} \tilde{\rho}(g_v)(\rho(g_v)^*)^{-1} \in H_2(G, c, \mathbb{Z}).$$

This invariant is independent of choice of  $\tilde{\rho}$ ,  $g_v$ , and  $I_v$ .

**Definition 4.5.** If  $L/K$  is a Galois extension with group  $G$ , we say that all ramification of  $L/K$  is of type  $c$  if  $L/K$  is tamely ramified, and for each prime  $\mathfrak{P}$  of  $L$ , either  $\mathfrak{P}$  is unramified, or else a generator of the inertia group at  $\mathfrak{P}$  is contained in  $c$ .

We consider Galois extensions  $L/K$  with Galois group  $G$  with the following properties:

- Conditions 4.6.** (1)  $G$  and  $c$  satisfy Conditions 4.1 above.  
 (2) All ramification of  $L/K$  is of type  $c$ .  
 (3)  $K$  and  $L$  are totally real number fields.

In the case where  $G = A_5$  and  $K = \mathbb{Q}$ , if  $c$  is the conjugacy class of 3-cycles so that  $H_2(G, c, \mathbb{Z}) \cong C_2$ , we can define the invariant in more down-to-earth terms. In this case,  $\tilde{G}_c = \tilde{A}_5$  and  $\tilde{c}$  is the conjugacy class of elements of order 3 in  $\tilde{G}_c$ .

**Claim 4.7.** *If  $L/\mathbb{Q}$  is the  $A_5$  field which is the fixed field of the kernel of  $\rho$  and  $\tilde{L}$  is the fixed field of the kernel of  $\tilde{\rho}$ , then the invariant  $\mathfrak{z}(\rho)$  is the number of primes  $p \equiv 3 \pmod{4}$  with even ramification index in  $\tilde{L}$ , modulo 2.*

*Proof.* We check the contribution to (4.1) at each prime. If  $\tilde{L}/L$  is unramified above  $v$ , then the contribution to the product is  $1 \in \{\pm 1\}$ . If  $v \equiv 3 \pmod{4}$  and  $\tilde{L}/L$  is ramified above  $v$ , then  $\tilde{\rho}(g_v)$  has even order in  $\tilde{G}_c$ , and  $\rho(g_v)^*$  has odd order, so the contribution to the product is  $-1$ . If  $v \equiv 1 \pmod{4}$  and  $\tilde{L}/L$  is ramified above  $v$ , then  $\tilde{\rho}(g_v)$  has odd order, as does  $\rho(g_v)^*$ , so they are equal. Hence in this case, the contribution to the product is 1. Thus, the product is  $-1$  to the number of primes congruent to 3 mod 4 which ramify in  $\tilde{L}/L$ . Since all ramified primes in  $L$  have odd ramification degree and all ramified primes in  $\tilde{L}/L$  have ramification degree 2, the claim is valid.  $\blacksquare$

**Remark 4.8.** The invariant is independent of the choice of  $\tilde{L}$ . Suppose we have another lift  $\tilde{L}'$ . Then  $\tilde{L}$  and  $\tilde{L}'$  differ by a totally real quadratic twist  $G_{\mathbb{Q}} \rightarrow C_2$  unramified at 2, and in any real quadratic field, the number of ramified primes congruent to 3 mod 4 is even.

In the case where  $G = A_4$  and  $K = \mathbb{Q}$ , we can take  $c$  to be the union of two conjugacy classes consisting of all 3-cycles of  $G$ . Then  $H_2(G, c, \mathbb{Z}) \cong C_2$ , and we take  $\tilde{G}_c = \tilde{A}_4$  and  $\tilde{c}$  the collection of elements of order 3 in  $\tilde{G}_c$ . The invariant is defined just like in the case of  $G = A_5$  above: if  $L/\mathbb{Q}$  is the  $A_4$  field over  $\mathbb{Q}$  which is the fixed field of a homomorphism  $\rho : G_{\mathbb{Q}} \rightarrow A_4$ , we can lift to an  $\tilde{A}_4$  field  $\tilde{L}$  which is tamely ramified and totally real. The invariant  $\mathfrak{z}(\rho)$  is again the number of primes  $p \equiv 3 \pmod{4}$  with even ramification index in  $\tilde{L}$ , modulo 2.

Much of the value of the invariant rests on our belief in the following conjecture:

**Conjecture 4.9.** *Assume Conditions 4.6 hold. As we vary  $L$  by discriminant,  $\mathfrak{z}(\rho)$  is equidistributed over  $H_2(G, c, \mathbb{Z})$ .*

**Remark 4.10.** We can think about  $A_4$  invariants in one of two ways. First, of course, they are invariants of  $A_4$  fields. But a totally real  $A_4$  field also corresponds to a Galois cubic field  $K$  together with a Galois-equivariant surjection  $\varphi : \text{Cl}(K) \rightarrow C_2 \times C_2$ : given such a field  $K$  and a surjection  $\varphi$ , we construct an unramified  $C_2 \times C_2$  cover  $H$  of  $K$ , so that  $H$  is Galois over  $\mathbb{Q}$  (and hence  $K$ ), with  $\text{Gal}(H/K) \cong C_2 \times C_2$  and  $\text{Gal}(H/\mathbb{Q}) \cong A_4$ . (This construction is described in section 5, and an example is given in detail in section 6.) Now, let  $c$  be the trivial conjugacy class in  $C_2 \times C_2$ . Although  $c$  does not generate  $C_2 \times C_2$ , the conclusion of Lemma 4.2 still holds. In this case, we have  $H_2(G, c, \mathbb{Z}) \cong C_2$ , so  $H$  lifts to fields  $\tilde{H}_1$  and  $\tilde{H}_2$ , with  $\text{Gal}(\tilde{H}_1/K) \cong D_8$  and  $\text{Gal}(\tilde{H}_2/K) \cong Q_8$  which are tamely ramified and totally real. Since the Sylow 2-subgroup of  $\tilde{A}_4$  is isomorphic to  $Q_8$ ,  $\tilde{H}_2$  is an  $\tilde{A}_4$ -field. If, furthermore, all ramification in  $H$  is of type 3-cycle, then  $\tilde{H}_2$  is a lift of  $H$  of the type described above. Hence, we can also think of the invariant associated to an  $A_4$  field  $H$  as being the invariant associated to a pair  $(K, \varphi)$ , where  $K$  is a  $C_3$  field and  $\varphi$  a surjection from  $\text{Cl}(K)$  to  $C_2 \times C_2$ .

## 5. COMPUTING THE INVARIANT

In this section, we present an algorithm that takes an  $A_4$  field ramified at one prime and produces an  $\tilde{A}_4$  lift of it. We then prove that the invariant associated to an  $A_4$  field is closely related to the class group; this will help us compute tables of invariants much more quickly than if we had to construct the  $\tilde{A}_4$  field in every case.

We are now in a position to calculate the invariant associated to a totally real  $A_4$  field  $H$ . Let  $c$  be set of all 3-cycles in  $A_4$ ; this is a union of two conjugacy classes in  $A_4$ . If  $H$  is ramified at exactly one prime, we will prove below that all ramification in  $H$  is of type  $c$ , so Lemma 4.2 tells us that we can lift  $H$  to a tamely ramified and totally real extension  $\tilde{H}$  with Galois group  $\tilde{A}_4 \cong \text{SL}_2(\mathbb{F}_3)$ . If  $H$  is ramified at more than one prime, all we can say is that the ramification of *some* prime is of type  $c$ .

**Proposition 5.1.** *If  $E/\mathbb{Q}$  is an  $A_4$  field ramified at exactly one rational prime, then all ramification is of type 3-cycle.*

This follows quickly from the following more general Lemma:

**Lemma 5.2.** *If  $E/\mathbb{Q}$  is a finite Galois extension with Galois group  $G$ , then the inertia groups at the ramified finite places of  $E$  generate  $G$ .*

*Proof.* Let  $E_0$  be the intersection of the fixed fields of all the inertia groups. Then  $E_0/\mathbb{Q}$  is a finite Galois extension unramified at all finite places. Hence  $E_0 = \mathbb{Q}$ , and so the inertia groups generate  $G$ . ■

*Proof of Proposition.* There are no wildly ramified  $A_4$  extensions of  $\mathbb{Q}$  ramified at exactly one rational prime (see [Jon]), so  $E$  must be tamely ramified. Hence, its ramification type must either be that of 3-cycles, or that of products of two disjoint 2-cycles. The latter case cannot happen by Lemma 5.2, because the products of two disjoint 2-cycles do not generate  $A_4$ . ■

Now, we shall see how to lift a totally real  $A_4$  field  $H$  ramified at exactly one rational prime to a tamely ramified and totally real  $\tilde{A}_4$  field  $\tilde{H}$ . Note that, since  $\tilde{H}/H$  will be a quadratic extension, tamely ramified is equivalent to being unramified above 2.

### Algorithm 5.3

**Input:** A quartic polynomial  $f$  defining a quartic field  $L$  with Galois closure a totally real  $A_4$  field  $H$  ramified at exactly one prime.

**Output:** An element  $\alpha \in L$  so that  $L(\sqrt{\alpha})$  has Galois closure an  $\tilde{A}_4$  field  $\tilde{H}$ , and so that  $\tilde{H}$  is totally real and tamely ramified.

1. Let  $\{\alpha_i\}$  be a set of representatives of  $\mathfrak{o}_L^\times / \mathfrak{o}_L^{\times 2}$  which includes 1.
2. Let  $\{C_j\}_{j \in J}$  be the 2-torsion ideal classes of  $L$ .
3. For  $j \in J$ , let  $I_j$  denote an integral ideal in  $C_j$ . Let the ideal (1) be the representative of the trivial ideal class.
4. Each  $I_j^2$  is a principal ideal; let  $\beta_j$  be a generator for  $I_j^2$ .
5. Let  $\gamma_1 = 1$ .
6. Let  $p$  be the rational prime at which  $L$  is ramified. Then  $p\mathfrak{o}_L$  splits as  $\mathfrak{p}_1\mathfrak{p}_2^3$ , for some prime ideals  $\mathfrak{p}_1, \mathfrak{p}_2 \subset \mathfrak{o}_L$ . Let  $J = \mathfrak{p}_1\mathfrak{p}_2$ . Suppose that the order of  $J$  in the class group is  $r$ . Let  $\gamma_2$  be a generator for the principal ideal  $J^r$ .
7. Let  $\Delta = \{\alpha_i\beta_j\gamma_k\}$ .
8. For  $\delta \in \Delta$ , check if  $L(\sqrt{\delta})$  has Galois group  $\tilde{A}_4$ . Stop once we have found one that does, and call this element  $\delta$ .
9. If  $L(\sqrt{\delta})$  is tamely ramified and totally real, let  $\alpha = \delta$ .
10. If  $L(\sqrt{\delta})$  is tamely ramified and totally complex, let  $q$  be a rational prime with  $q \equiv 3 \pmod{4}$  so that  $L(\sqrt{\delta})$  is unramified at  $q$ . Let  $\alpha = -q\delta$ .
11. If  $L(\sqrt{\delta})$  is wildly ramified and totally real, let  $q$  be a rational prime with  $q \equiv 3 \pmod{4}$  so that  $L(\sqrt{\delta})$  is unramified at  $q$ . Let  $\alpha = q\delta$ .
12. If  $L(\sqrt{\delta})$  is wildly ramified and totally complex, let  $\alpha = -\delta$ .
13. Return  $\alpha$ .

*Proof of Algorithm 5.3.* By Lemma 4.2, we know that there is an  $\alpha \in H$  so that  $H(\sqrt{\alpha})$  is Galois over  $\mathbb{Q}$  with Galois group  $\tilde{A}_4$ . Suppose we have such an  $\alpha$ . Let  $q$  be a rational prime different from  $p$ , and let  $q\mathfrak{o}_H = \mathfrak{q}_1 \cdots \mathfrak{q}_g$ . In order for  $H(\sqrt{\alpha})$  to be Galois over  $\mathbb{Q}$  it is necessary and sufficient that the class of  $\alpha$  in  $H^\times/H^{\times 2}$  is stable under the action of  $\text{Gal}(H/\mathbb{Q})$ . If the class of  $\alpha$  in  $H^\times/H^{\times 2}$  is  $\text{Gal}(H/\mathbb{Q})$ -stable, then the parity of  $v_{\mathfrak{q}_i}(\alpha)$  must be the same for all  $i$ . If  $v_{\mathfrak{q}_i}(\alpha) \equiv 1 \pmod{2}$  for all  $i$  and the class of  $\alpha$  is  $\text{Gal}(H/\mathbb{Q})$ -stable, then  $v_{\mathfrak{q}_i}(\alpha/q) \equiv 0 \pmod{2}$  for all  $i$ , and the class of  $\alpha/q$  is still  $\text{Gal}(H/\mathbb{Q})$ -stable. Hence, we may assume that  $v_{\mathfrak{q}}(\alpha) \equiv 0 \pmod{2}$  for all primes  $\mathfrak{q}$  of  $H$  lying over a rational prime different from  $p$ . Furthermore, the parities of  $v_{\mathfrak{p}_i}(\alpha)$  are equal for all primes  $\mathfrak{p}_i$  of  $H$  lying over  $p$ . Let  $\Xi$  be the set of square classes of  $H$  with even valuation at all primes not lying over  $p$ , and with all valuations at primes over  $p$  having the same parity.

Let  $B$  be the kernel of the map  $\tilde{A}_4 \twoheadrightarrow A_4$ . Then  $\tilde{A}_4$  acts transitively and faithfully on a set of 8 objects partitioned into blocks of size 2 so that  $B$  fixes the blocks. The quotient  $A_4 \cong \tilde{A}_4/B$  acts on the blocks in the usual way that  $A_4$  acts on 4 objects. Hence any  $\tilde{A}_4$  field is the Galois closure of an octic field obtained by adjoining the square root of some square class in a quartic field. Hence, we may restrict our list of square classes to check still further by letting  $\Delta$  be the set of square classes in  $\Xi$  which contain a representative in  $L$ . This shows that we can find a  $\delta$  in Step 8 so that  $L(\sqrt{\delta})$  has Galois group  $\tilde{A}_4$ .

The remaining steps explain how we can twist by a quadratic character in order to remove wild ramification and ramification at  $\infty$ . Let  $\tilde{\rho} : G_{\mathbb{Q}} \rightarrow \tilde{A}_4$  be the Galois representation corresponding to the number field  $H(\sqrt{\delta})$ . We can find some quadratic character  $\chi : G_{\mathbb{Q}} \rightarrow C_2$  so that the representation  $\chi\tilde{\rho}$  is tamely ramified and unramified at  $\infty$ . This completes the proof.  $\blacksquare$

Once we have found the desired  $\tilde{L}$ , we can simply count the number of ramified primes congruent to 3 (mod 4) in  $\tilde{L}$  in order to determine the invariant  $\mathfrak{z}(\rho)$ .

Frequently, it is possible to compute the invariant without constructing an explicit lift to an  $\tilde{A}_4$  field. (Still, as a matter of good discipline and for the sake of generality, it is good to know how to perform the explicit construction.) We recall that  $\text{Cl}_2(K)$  denotes the Sylow 2-subgroup of  $\text{Cl}(K)$ . We define variants such as  $\text{Cl}_2^+(K)$  to mean the Sylow 2-subgroup of  $\text{Cl}^+(K)$ , and in general, a subscript of 2 in any sort of class group will denote the Sylow 2-subgroup of that class group. In the situation at hand, we have the following characterization of the invariant:

**Theorem 5.4.** *Let  $K$  be a  $C_3$  field with prime conductor so that  $\text{Cl}_2(K) \cong C_2 \times C_2$ , and let  $H$  be the everywhere unramified  $C_2 \times C_2$  extension of  $K$ , so that  $H$  is an  $A_4$  field. Let  $L \subset H$  be the fixed field of any 3-cycle in  $\text{Gal}(H/\mathbb{Q})$ , so that  $L$  is a non-Galois quartic field over  $\mathbb{Q}$  with Galois closure  $H$ . Suppose furthermore that  $\text{Cl}_2^+(L)$  is cyclic. Then the invariant associated to  $H$  is equal to  $\#\text{Cl}(L) \pmod{2}$ .*

*Proof.* By the above, we have an  $\tilde{A}_4$  field  $\tilde{H}$  containing  $H$  so that  $\tilde{H}$  is totally real and tamely ramified. While the construction of  $\tilde{H}$  is not unique, any two such  $\tilde{H}$ 's differ only by a quadratic twist  $\chi : G_{\mathbb{Q}} \rightarrow C_2$ . Let  $\tilde{\rho} : G_{\mathbb{Q}} \rightarrow \tilde{A}_4$  be the Galois representation associated to one such  $\tilde{H}$ . Suppose that  $\tilde{H}/H$  were ramified at two primes of  $H$  above two distinct primes  $p_1$  and  $p_2$  of  $\mathbb{Q}$ , so that  $p_1 \equiv p_2 \equiv 3 \pmod{4}$ . Let  $\chi : G_{\mathbb{Q}} \rightarrow C_2$  be the quadratic character associated to the number field  $\mathbb{Q}(\sqrt{p_1 p_2})$ . Then the number field associated to the representation  $\chi \tilde{\rho}$  is again an  $\tilde{A}_4$  field which is still tamely ramified, totally real, and contains  $H$ , and the corresponding quadratic extension of  $H$  is ramified at exactly the primes at which  $\tilde{H}$  ramifies, with the exception of the primes above  $p_1$  and  $p_2$ , where it is now unramified. Similarly, if  $\tilde{H}/H$  were ramified at a prime in  $H$  above some rational prime  $q \equiv 1 \pmod{4}$ , then if  $\chi$  is the quadratic character associated to  $\mathbb{Q}(\sqrt{q})$ , then the number field associated to the representation  $\tilde{\rho} \chi$  is now unramified at the primes above  $q$ . Hence, we may assume that there are no primes congruent to 1 (mod 4) for which the primes in  $H$  above  $p$  are ramified in  $\tilde{H}/H$ , and there is at most one such prime congruent to 3 (mod 4). If we have a prime  $q \equiv 3 \pmod{4}$  for which the primes above  $q$  are ramified in  $\tilde{H}/H$ , let  $\chi$  be the quadratic character associated to  $\mathbb{Q}(\sqrt{-q})$ . Then the field associated to  $\chi \tilde{\rho}$  is unramified at the primes above  $q$  in  $H$ .

The above paragraph shows us how to produce a quadratic extension  $\tilde{H}/H$  unramified at all finite places, so that  $\text{Gal}(\tilde{H}/\mathbb{Q}) \cong \tilde{A}_4$ . By the argument in the proof of Algorithm 5.3,  $\tilde{H}$  descends to a quadratic extension  $\tilde{L}$  of  $L$ , unramified at all finite places, so that the Galois closure of  $\tilde{L}$  over  $\mathbb{Q}$  is  $\tilde{H}$ . Hence,  $\text{Cl}_2^+(L)$  is nontrivial. If  $\text{Cl}_2^+(L)$  is cyclic, then there is a *unique* nontrivial quadratic extension of  $L$  unramified at all finite places, so this extension must be  $\tilde{L}$ . In this case,  $\tilde{L}$  and hence  $\tilde{H}$  are totally real if and only if  $\text{Cl}_2(L)$  is nontrivial. If this happens, then  $\tilde{H}/H$  is everywhere unramified (including at infinity), so the invariant is 0. If  $\text{Cl}_2(L)$  is trivial, then  $\tilde{H}/H$  is ramified only at infinity, so we can twist by some character associated to a field  $\mathbb{Q}(\sqrt{-p})$  for some  $p \equiv 3 \pmod{4}$  to obtain a totally real  $\tilde{H}$  ramified only at  $p$ . Hence, the invariant in this case is 1. In either case, the invariant is  $\# \text{Cl}_2(L) \pmod{2}$ . ■

**Remark 5.5.** The hypothesis that  $\text{Cl}_2^+(L)$  is cyclic holds very frequently. In fact, there are no exceptions in the  $10^5$  fields we tested for inclusion in the data given in Table 1.

In §6, we will need to start with a  $C_3$  field  $K$  with  $\text{Cl}_2(K) \cong C_2 \times C_2$  and construct an  $A_4$  field  $H$  containing  $K$  so that  $H/K$  is everywhere unramified. We now explain how that is done.

### Algorithm 5.6

**Input:** A cubic polynomial  $f$  defining a Galois cubic field  $K$ .

**Output:** A quartic polynomial  $g$  so that the Galois closure of  $g$  is an  $A_4$  field  $H$  containing  $K$ , with  $H/K$  everywhere unramified.

1. Let  $\{\alpha_i\}$  be a set of representatives of  $\mathfrak{o}_K^\times / \mathfrak{o}_K^{\times 2}$ .
2. Let  $\{C_j\}_{j \in J}$  be the 2-torsion ideal classes of  $K$ .
3. For  $j \in J$ , let  $I_j$  denote an integral ideal in  $C_j$ . Let the ideal (1) be the representative of the trivial ideal class.
4. Each  $I_j^2$  is a principal ideal; let  $\beta_j$  be a generator for  $I_j^2$ .
5. Let  $\Delta = \{\alpha_i \beta_j\}$ .
6. For  $\delta \in \Delta$ , let  $K_\delta$  be the Galois closure over  $\mathbb{Q}$  of  $K(\sqrt{\delta})$ . If  $K_\delta$  has Galois group  $A_4$  and is totally real and unramified at 2, let  $\alpha = \delta$  and stop.
7. Let  $x^3 - a_2x^2 + a_1x - a_0$  be the minimal polynomial of  $\alpha$  over  $\mathbb{Q}$ .
8. Let  $b_2 = -2a_2$ ,  $b_1 = -8\sqrt{a_0}$ ,  $b_0 = a_2^2 - 4a_1$ .
9. Let  $h(x) = x^4 + b_2x^2 + b_1x + b_0$ .
10. (Optional.) Using the LLL algorithm, find a polynomial  $g$  with smaller coefficients than  $h$  so that  $g$  and  $h$  generate the same field; this is implemented in PARI/GP [The08] as `polredabs`.
11. Return  $g$ .

*Proof of Algorithm 5.6.* We first show that there is some  $\alpha \in \Delta$  so that the Galois closure  $H$  of  $K(\sqrt{\alpha})$  has Galois group  $A_4$  over  $\mathbb{Q}$  and so that  $H/K$  is everywhere unramified. By class field theory, we know that there is some such  $\alpha \in K^\times$ , so it suffices to show that if  $\alpha \notin \Delta K^{\times 2}$ , then  $K(\sqrt{\alpha})/K$  is ramified somewhere. Observe that for  $K(\sqrt{\alpha})/K$  to be unramified, it is necessary (but not sufficient) that  $\alpha$  have even valuation at all places of  $K$ . Those elements of  $K^\times$  which have even valuation at all places of  $K$  are precisely the elements of  $\Delta K^{\times 2}$ , so this shows that we can find such an  $\alpha \in \Delta$ .

Now we explain the construction of  $h(x)$ . The  $A_4$  field  $H$  is the Galois closure of a quartic field  $L$  over  $\mathbb{Q}$ . Since  $\alpha$  has degree 3 over  $\mathbb{Q}$  and is not a square,  $\sqrt{\alpha}$  has degree 6. Let us call its Galois conjugates  $\pm\sqrt{\alpha}, \pm\sqrt{\beta}, \pm\sqrt{\gamma}$ . Now,  $L$  is generated by  $r = \sqrt{\alpha} + \sqrt{\beta} + \sqrt{\gamma}$ . The conjugates of  $r$  are  $r_2 = \sqrt{\alpha} - \sqrt{\beta} - \sqrt{\gamma}$ ,  $r_3 = -\sqrt{\alpha} + \sqrt{\beta} - \sqrt{\gamma}$ , and  $r_4 = -\sqrt{\alpha} - \sqrt{\beta} + \sqrt{\gamma}$ , and so we can check explicitly that  $h$  as constructed in Algorithm 5.6 is the minimal polynomial of  $r$ .  $\blacksquare$

Suppose now that  $K$  is a  $C_3$  field ramified at exactly one rational prime  $p$ . Then  $H$  as constructed in Algorithm 5.6 is also ramified at  $p$  and nowhere else. Furthermore,  $H$  is totally real.

## 6. A SAMPLE INVARIANT COMPUTATION

Let us compute the invariant for the smallest  $A_4$  field ramified at one prime. In order to build this  $A_4$  field, we start with the smallest  $C_3$  field with prime conductor and class group  $C_2 \times C_2$ . A polynomial generating this field is  $p(x) = x^3 - x^2 - 54x + 169$ ; the field is ramified only at 163. Let  $K$  denote this field, and let  $\alpha$  be a root of  $p$  in  $K$ . The unit group is

$$\mathfrak{o}_K^\times = (\alpha - 4)^\mathbb{Z} \times (\alpha^2 + 4\alpha - 33)^\mathbb{Z} \times \{\pm 1\}.$$

Two ideals whose ideal classes generate the class group are  $(5, \alpha - 2)$  and  $(5, \alpha - 1)$ , and the squares of these ideals are  $(\alpha^2 + 4\alpha - 32)$  and  $(\alpha^2 + 4\alpha - 35)$ , respectively.

To find the Hilbert class field of  $K$ , it suffices to look at  $K(\sqrt{\beta})$ , where  $\beta$  is the product of elements of some subset of  $\{-1, \alpha - 4, \alpha^2 + 4\alpha - 33, \alpha^2 + 4\alpha - 32, \alpha^2 + 4\alpha - 35\}$ . We find that, if  $\beta$  is one of  $\{\gamma_1, \gamma_2, \gamma_3\}$ , where  $\gamma_1 = \alpha^2 + 4\alpha - 32$ ,  $\gamma_2 = (\alpha - 4)(\alpha^2 + 4\alpha - 33)(\alpha^2 + 4\alpha - 35) = 12\alpha^2 + 48\alpha - 395$ , and  $\gamma_3 = (\alpha - 4)(\alpha^2 + 4\alpha - 33)(\alpha^2 + 4\alpha - 32)(\alpha^2 + 4\alpha - 35) = 169\alpha^2 + 688\alpha - 5612$ , then  $K(\sqrt{\beta})$  is an unramified extension of  $K$ . Hence, if  $\beta$  is one of these elements, then the Hilbert class field  $H(K)$  of  $K$  is the Galois closure of  $K(\sqrt{\beta})$ .

Now, we find an equation for a quartic field  $L$  whose Galois closure is  $H(K)$ . Take  $\beta$  as in the above paragraph, so that  $H(K)$  is the Galois closure of  $K(\sqrt{\beta})$ . Suppose the Galois conjugates of  $\beta$  in  $K$  are  $\beta_1 = \beta, \beta_2, \beta_3$ . Then the minimal polynomial of  $\sqrt{\beta}$  over  $\mathbb{Q}$  has roots  $\pm\sqrt{\beta_1}, \pm\sqrt{\beta_2}$ , and  $\pm\sqrt{\beta_3}$ . An example of a quartic polynomial with the same Galois closure has roots  $\sqrt{\beta_1} + \sqrt{\beta_2} + \sqrt{\beta_3}, \sqrt{\beta_1} - \sqrt{\beta_2} - \sqrt{\beta_3}, -\sqrt{\beta_1} + \sqrt{\beta_2} - \sqrt{\beta_3}$ , and  $-\sqrt{\beta_1} - \sqrt{\beta_2} + \sqrt{\beta_3}$ . A polynomial with these roots is  $x^4 - 34x^2 - 40x + 121$ . Using the PARI/GP function `polredabs`, we find that another polynomial that generates the same field is  $f(x) = x^4 - x^3 - 7x^2 + 2x + 9$ . Let  $L$  be the field  $\mathbb{Q}[x]/(f(x))$ , and let  $\gamma$  be a root of  $f$  in  $L$ .

Now, we must construct a degree-8 extension of  $L$  whose Galois group is isomorphic to  $\tilde{A}_4$ . First, we must find generators for the unit group of  $L$ . The unit group of  $L$  is isomorphic to  $\mathbb{Z}^3 \times \{\pm 1\}$ , and a basis for the torsion-free part is  $\{\gamma^2 - 2, \gamma + 2, \gamma^2 - 2\gamma - 4\}$ . The class group of  $L$  is trivial, so we get no contribution from 2-torsion ideal classes. Finally,  $L$  is ramified exactly at the prime 163, and  $(163)$  factors as  $\mathfrak{p}_1\mathfrak{p}_2^3$ , where  $\mathfrak{p}_1 = (\gamma^3 - 4\gamma - 4)$  and  $\mathfrak{p}_2 = (-4\gamma^3 + 9\gamma^2 + 16\gamma - 26)$ . Hence,  $\mathfrak{p}_1\mathfrak{p}_2 = (6\gamma^3 - 11\gamma^2 - 23\gamma + 23)$ . Thus, some field of the form  $L(\sqrt{\delta})$ , where  $\delta$  is the product of elements of some subset of  $\{\gamma^2 - 2, \gamma + 2, \gamma^2 - 2\gamma - 4, 6\gamma^3 - 11\gamma^2 - 23\gamma + 23\}$ , has Galois group  $\tilde{A}_4$ . We find that, if  $\delta = \gamma + 2$ , then the Galois closure of  $L_1 = L(\sqrt{\delta})$  has Galois group  $\tilde{A}_4$  over  $\mathbb{Q}$ . Now,  $L_1$  is totally real, but it is ramified at 2, and hence not tamely ramified. Thus, we need to twist by a character that is ramified at one prime congruent to 3 (mod 4). In particular,  $L_2 = L(\sqrt{3\delta})$  has Galois group  $\tilde{A}_4$ , is totally real, and is tamely ramified, so it is a lift of the desired form. Now, in order to compute  $\mathfrak{z}(\rho)$ , we need to determine the number of primes congruent to 3 (mod 4) that are ramified to even order. There are two ramified primes of  $L_2$ , namely 3 and 163. Only 3 is ramified to even order, so  $\mathfrak{z}(\rho) = 1$ .

This computation, and all others in this paper, were done using Sage [S<sup>+</sup>10] and PARI/GP [The08].

## 7. THE DATA

We collected data from the first  $10^5$   $C_3$  fields  $K$  ramified at exactly one prime such that the Sylow 2-subgroup of the class group of  $K$  is isomorphic to  $C_2 \times C_2$  and constructed the associated  $A_4$  fields. Of these, 53891 have invariant 1 and 46109

TABLE 1. Invariant Data

$N$	Invariant 1	Proportion with invariant 1
100	55	.5500
200	104	.5200
300	160	.5333
400	212	.5300
500	266	.5320
1000	536	.5360
2000	1063	.5315
4000	2183	.5458
6000	3279	.5465
8000	4372	.5465
10000	5456	.5456
20000	10862	.5431
30000	16267	.5422
40000	21638	.5410
50000	27064	.5413
60000	32400	.5400
70000	37768	.5395
80000	43176	.5397
90000	48578	.5398
100000	53891	.5389

have invariant 0. So, while we might be forgiven for expecting that the invariant equidistributes among the two classes, the data seem to exhibit a slight bias that gradually goes away. Table 1 gives incremental data for the invariants.

The first column denotes the number of fields, the second denotes the number with invariant 1, and the third denotes the proportion with invariant 1. Hence, we suspect, somewhat hesitantly, that the two classes do equidistribute, but that there is a secondary term of slightly lower order that leads to an apparent bias that persists for a long time. Based on the numerical evidence, and the fact that the number of cubic fields with absolute value of the discriminant at most  $x$  is of the form

$$ax + bx^{5/6} + o(x^{5/6})$$

for certain explicitly known constants  $a$  and  $b$  (see [BST10] and [TT11]), we might conjecture that the proportion of these  $C_3$  fields with invariant 1 among the first  $x$  by discriminant is

$$1/2 + cx^{-1/6} + o(x^{-1/6}),$$

where  $c \approx 0.27$ , perhaps with some logarithms thrown in because we are parametrizing fields in a slightly different manner from [BST10] and [TT11]. Still, there is not yet



enough data to be able to distinguish between an error term of the form  $cx^{-1/6}$  and, perhaps,  $c'x^{-1/8}$ , so this conjecture ought to be taken with more than a grain of salt.

### ACKNOWLEDGMENTS

I would like to thank my advisor, Akshay Venkatesh, for suggesting this problem to me and for providing me with a large amount of insight and wisdom. In addition, I am grateful to Jordan Ellenberg, Silas Johnson, Jürgen Klüners, Hendrik Lenstra, Carl Pomerance, David Roberts, and Craig Westerland for their useful remarks and suggestions.

### REFERENCES

- [Bil95] P. Billingsley. *Probability and measure*. Wiley Series in Probability and Mathematical Statistics. John Wiley & Sons Inc., New York, third edition, 1995. A Wiley-Interscience Publication.
- [BST10] M. Bhargava, A. Shankar, and J. Tsimerman. On the Davenport-Heilbronn theorem and second order terms. 2010. <http://arxiv.org/abs/1005.0672>.
- [CL84] H. Cohen and H. W. Lenstra, Jr. Heuristics on class groups of number fields. In *Number theory, Noordwijkerhout 1983 (Noordwijkerhout, 1983)*, volume 1068 of *Lecture Notes in Math.*, pages 33–62. Springer, Berlin, 1984.
- [CM87] H. Cohen and J. Martinet. Class groups of number fields: numerical heuristics. *Math. Comp.*, 48(177):123–137, 1987.
- [CM90] H. Cohen and J. Martinet. Étude heuristique des groupes de classes des corps de nombres. *J. Reine Angew. Math.*, 404:39–76, 1990.
- [EVW09] J. S. Ellenberg, A. Venkatesh, and C. Westerland. Homological stability for hurwitz spaces and the cohen-lenstra conjecture over function fields. 2009. <http://arxiv.org/abs/0912.0325v2>.
- [EVW12] J. S. Ellenberg, A. Venkatesh, and C. Westerland. Homological stability for Hurwitz spaces and the Cohen-Lenstra conjecture over function fields, II. 2012.
- [FT93] A. Fröhlich and M. J. Taylor. *Algebraic number theory*, volume 27 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 1993.
- [Jon] J. Jones. Number fields. <http://hobbes.la.asu.edu/NFDB/>.
- [Kar87] G. Karpilovsky. *The Schur multiplier*, volume 2 of *London Mathematical Society Monographs. New Series*. The Clarendon Press Oxford University Press, New York, 1987.
- [Mal08] G. Malle. Cohen-Lenstra heuristic and roots of unity. *J. Number Theory*, 128(10):2823–2835, 2008.
- [RS12] S. Rubinstein-Salzedo. Controlling ramification in number fields. 2012. <http://www.math.dartmouth.edu/~simon/thesis.pdf>.
- [S<sup>+</sup>10] W. A. Stein et al. *Sage Mathematics Software (Version 4.5.1)*. The Sage Development Team, 2010. <http://www.sagemath.org>.
- [The08] The PARI Group, Bordeaux. *PARI/GP, version 2.3.3*, 2008. available from <http://pari.math.u-bordeaux.fr/>.
- [TT11] T. Taniguchi and F. Thorne. Secondary terms in counting functions for cubic fields. 2011. <http://arxiv.org/abs/1102.2914>.
- [VE10] A. Venkatesh and J. S. Ellenberg. Statistics of number fields and function fields. In *Proceedings of the International Congress of Mathematicians. Volume II*, pages 383–402, New Delhi, 2010. Hindustan Book Agency.

DEPARTMENT OF MATHEMATICS, DARTMOUTH COLLEGE, HANOVER, NH 03755

*E-mail address:* `simon.rubinstein-salzedo@dartmouth.edu`